DMDC Days

DMDC Enterprise Web Services

Sept 18-20, 2012

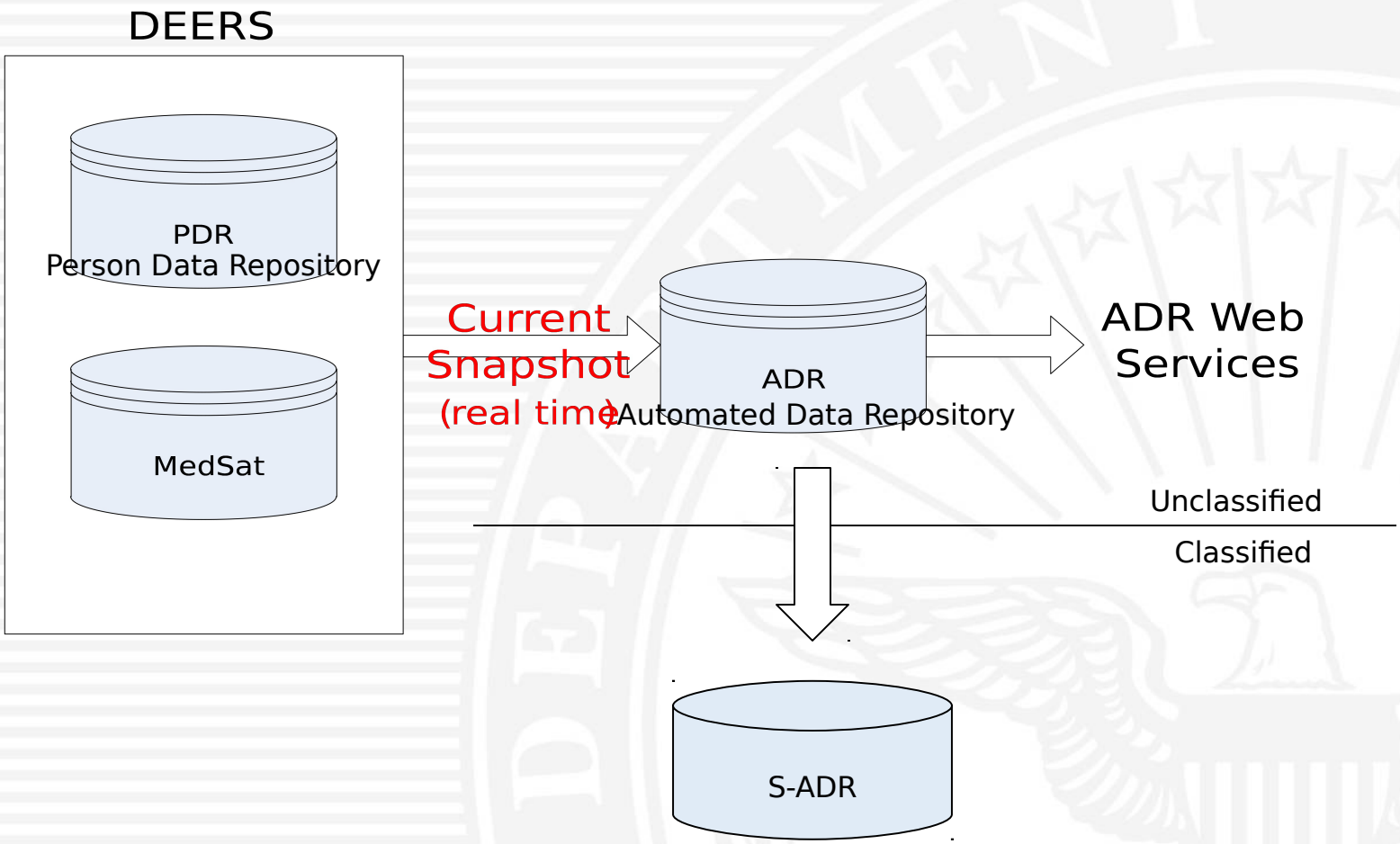
Lynne Prince, DMDC Enterprise Services Divsion

Serving Those Who Serve Our Country

Enterprise Web Services

- **Web Services**
  - Real Time Broker Service(RBS)/Batch Broker Service(BBS) -Account provisioning, identity and token validation, benefits and eligibility determination
  - DoD Enterprise Email
- **Global Force Management – Data Initiative** (GFM-DI) -
  - Prototype with AF/A5XW – ‘faces to spaces’
- **Attribute Based Access Control (ABAC)** – real time access control using authoritative attribute sources
  - Enterprise Identity Attribute Service (EIAS) – Service for Authoritative Identity Attributes

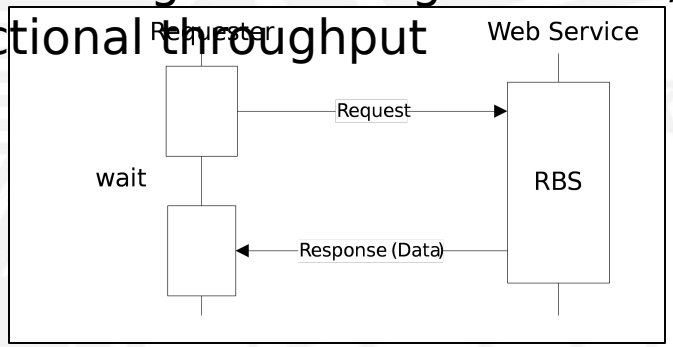
DMDC Web Services



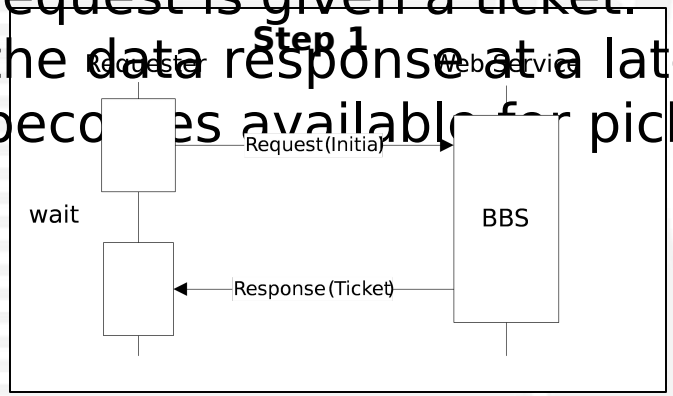
Core Web Services

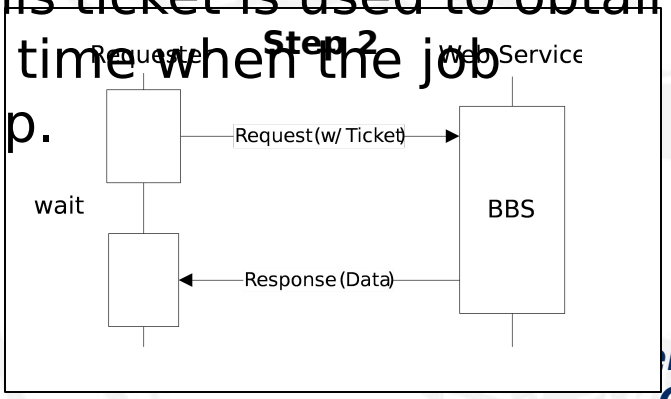
Synchronous – real time response to an inquiry

Synchronous services are designed for high-volume, high-speed, real-time transactional throughput

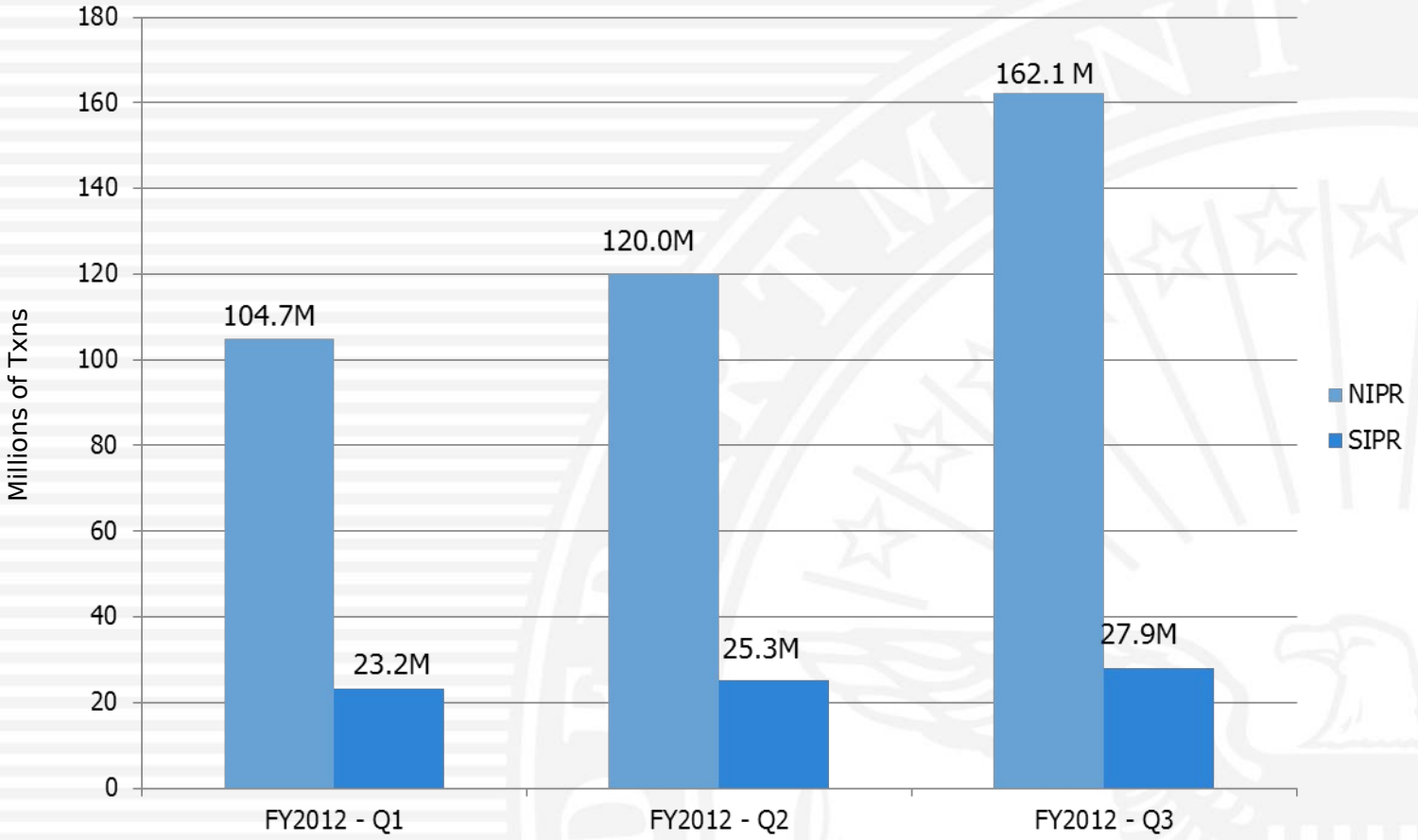


Asynchronous - is a two-step request. An initial request is given a ticket. This ticket is used to obtain the data response at a later time when the job becomes available for pickup.

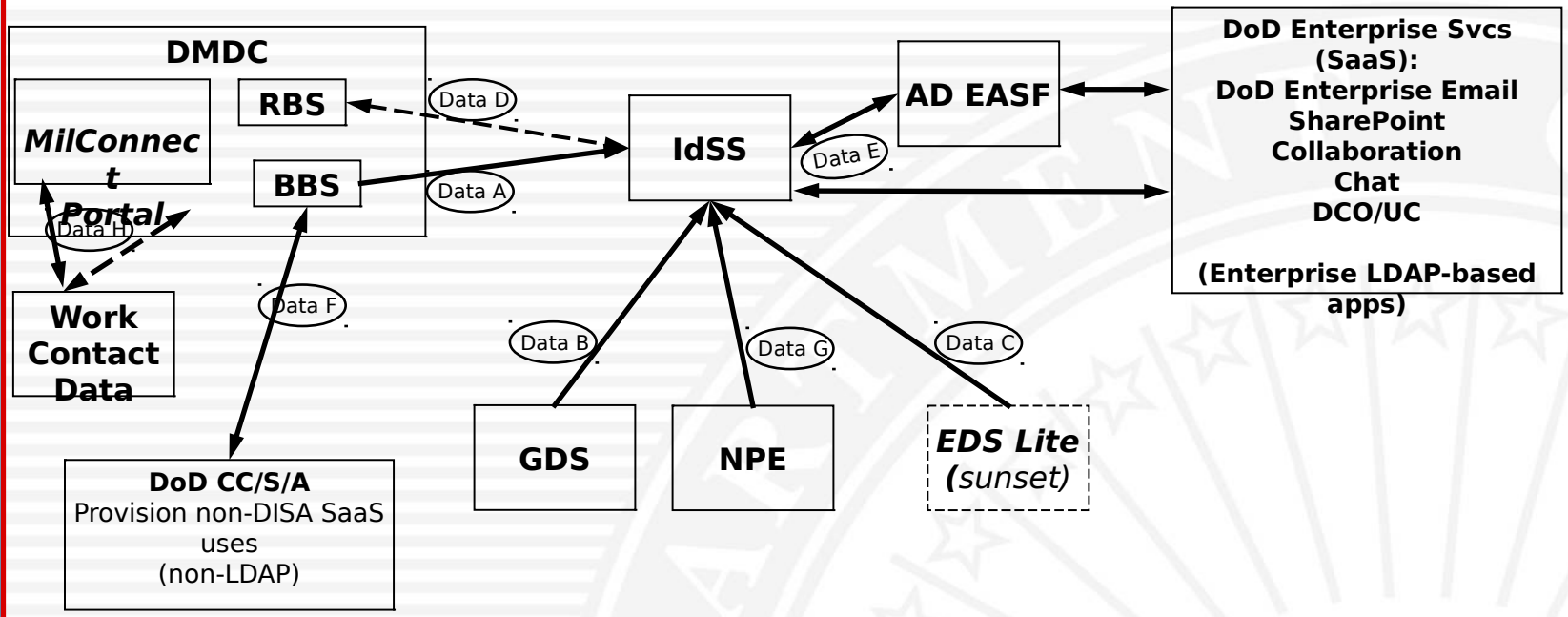




DMDC Web Services Transactions



DoD Enterprise Email Web Service



Data A – person & persona data, primary path for data to IdSS

Data B – encryption certificate, other certificate data;rare scenario: email addr

Data C – Army user work contact data not available in DEERS (short term), such as IT entitlements - replace with Milconnect data – update work contact info

Data D – if needed to reconcile data (generally equal to Data A)

Data E – data compiled from inputs and generated by IdSS in AD/LDAP

Data F – Enterprise provisioning services for the Department

Data G – Non-Person Entity data

Data H – Work Contact data – initial seed and on going

DoD Enterprise Email

- Consists of Enterprise User Name + Persona Type Code Name.PersonaType@mail.mil
  - Lynne.Prince4.CIV@mail.mil
  - GAL
  - White Pages
- Use MilConnect to:
  - Update Work Contact Information
  - Add a Preferred Name
  - Choose a Duty Organization, Sub Organization, and Installation
- Use RAPIDS Self Service (RSS)
  - Update your Email Certificate with your new Email Address
- Changes to MLA/RSS addresses
- Changes to Outlook objects: Global Calendars, Joint Task Lists etc..

Global Force Management - Data Initiative - CONOPS

Electronically documents "Authorized" force structure data for integration across DoD

Feeder Systems

eJMAPS
TFSMS DRRS-N
FMS GCSS-AF

Raw Data

ORG Servers "Shared"

Types of Data
Billet
Organization
Command
elationship
s

AIR FORCE
ARMY
MARINE CORPS
NAVY
Intel Community
OSD
JOINT STAFF

Force Structur
DOD
USA USAF USN USMC
States
ANG ARNG

Billet Data
-Rank/Grade
-MOS/AFSC
-Skill Code
-Skill Level
-Service
-Effective Date
-Service Billet ID

Elements tagged with unique identifiers per DODD 8320.3
Apply Organizational & Force Structure Construct (OFSC)
– Document hierarchies & command/support relationships (per the Service's Title 10 responsibilities)

Net-Centric Enterprise Services

Content Discovery Core
Enterprise Service
Metadata Registry
NCES Service Registry

Visible

GFM Informati on Exchange Schema

Accessible

Web Services
Publish/Subscribe
IAW Net-Centric Data Strategy

Authoritative Force Structure Data

Understandabl

Data Consumers

PPBE
DoD HR
DRRS

BFT
DMDA
Readines

Force Employm
Adaptive Planning
GUID Registry

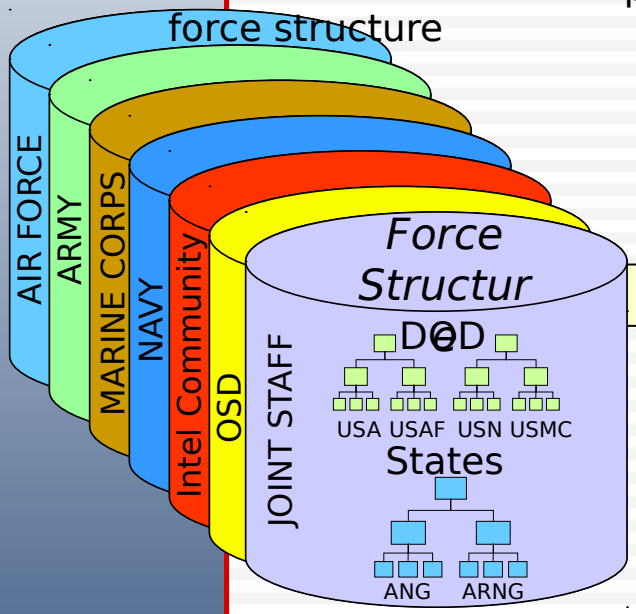
Intelligence
C2 Systems
Installations

Personnel
Financial
Logistics

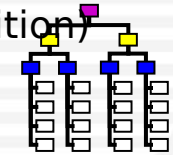
Initialization Data
Analytic Agenda
Battle C2 Systems

J8 – DMDC – Services/Agencies Linkage

1. Org Servers are Attribute Data Server for authoritative authorized force structure

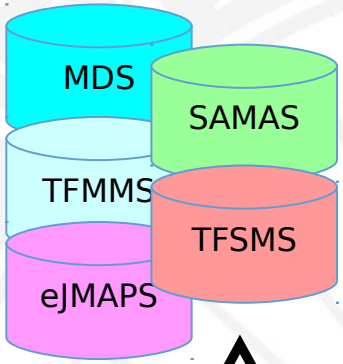


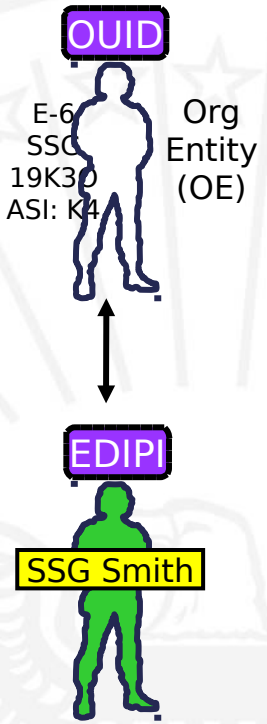
2. Force structure provided in common format (GFM XMLSchema Definition)

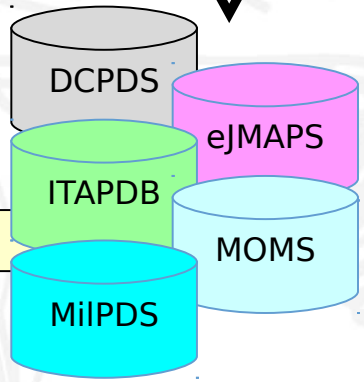


3. Using DoD approved publish and subscribe messaging service (Joint User Messaging (JUM)) for consumption by authorized users

4. Component manpower systems use/incorporate GFM DI authorized force structure (command structure and relationships to existing component representations)





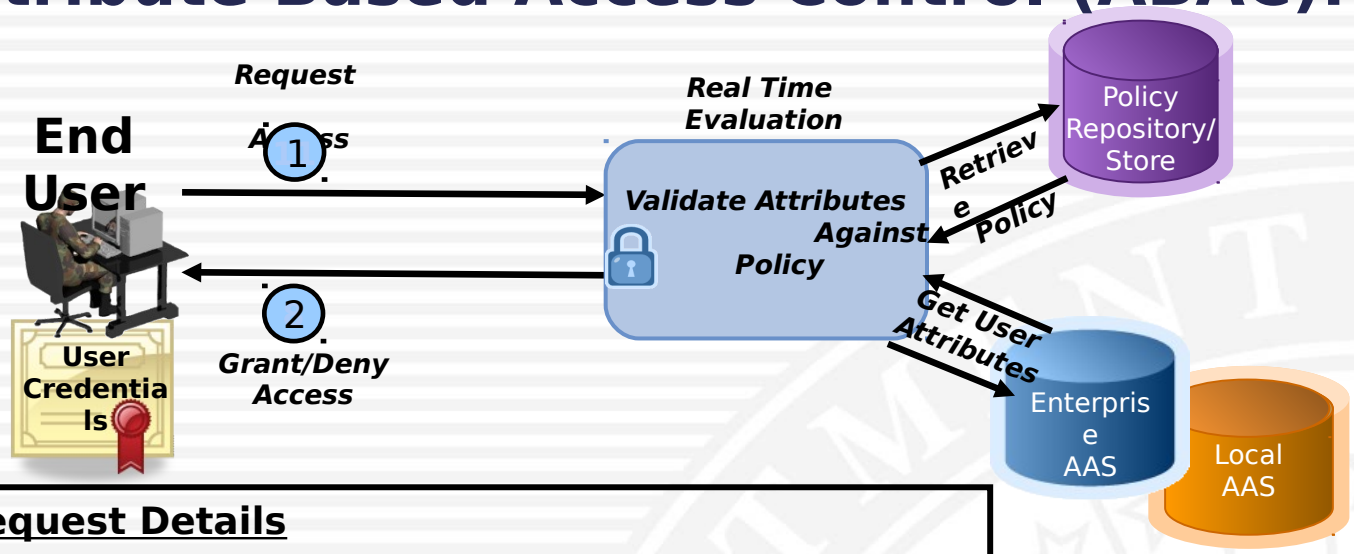


5. Link and maintain the billet-level OUID-to-EDIPI relationship

6. Expose the OUID-to-EDIPI relationship link to authorized users via web service; minimum to OSD P&R DMDC

Billet Data
- *Rank/Grade*
- *MOS/AFSC*
- *Skill Code*
- *Skill Level*
- *Service*
- *Effective Date*
- *Service Billet ID*

Attribute Based Access Control (ABAC): The Ba



Request Details

- **Subject**
- **Resource (Target)**
- **Action**

Policy Enforcement Point (PEP): Controls access to resources based on policy decisions from the Policy Decision Point(PDP).

Policy Decision Point (PDP): Determines if access should be granted by comparing access policies with requestor attributes.

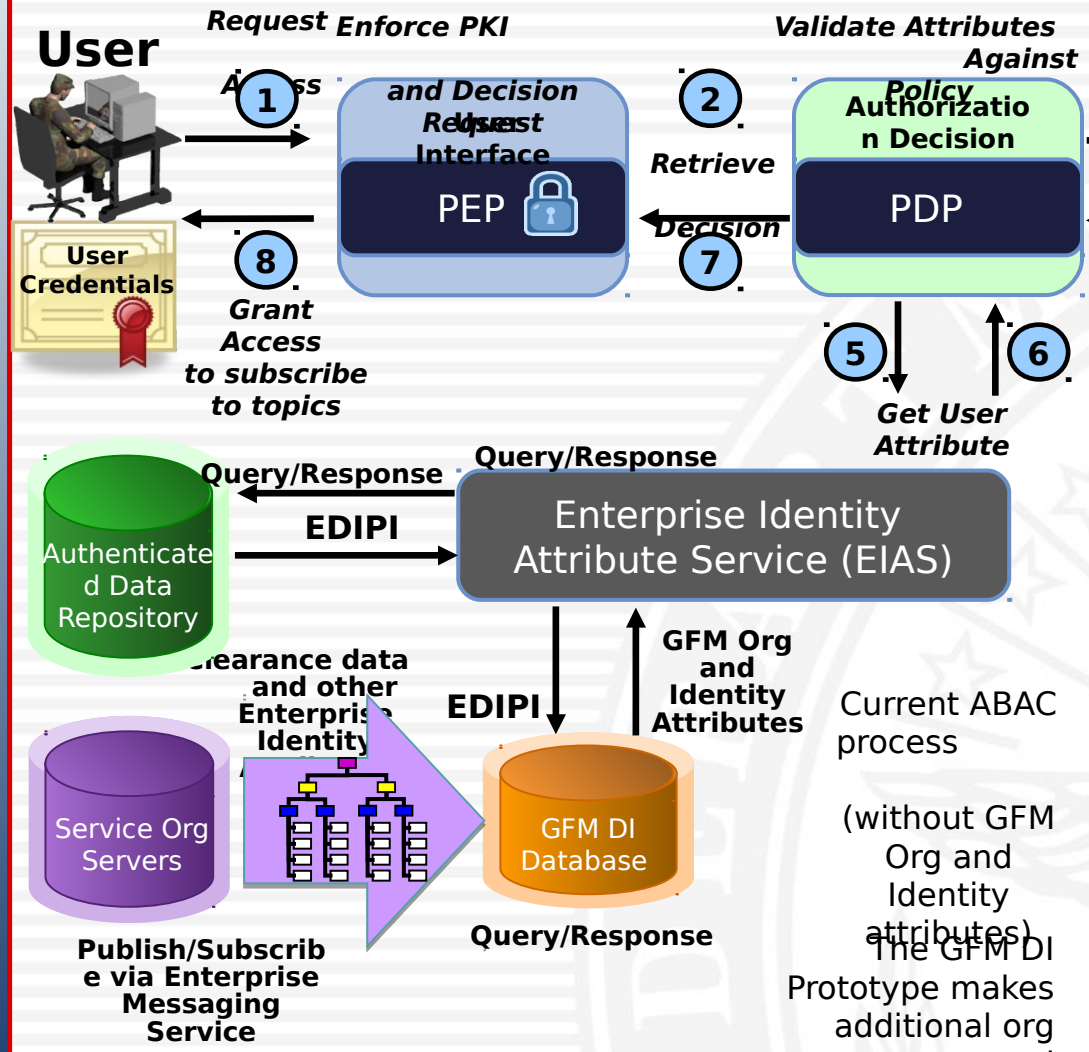
Policy Store: Contains pre-defined policies/policy sets which define the attributes necessary to access a particular resource.

Attribute Services: Web Services that provides access to attributes from one or more attribute sources.

Authoritative Attribute Source (AAS): Authoritative source of attributes available for ABAC decisions.

Attribute-Bases Access Control (ABAC)

GFM-DI and EIAS



Current ABAC process

(without GFM Org and Identity attributes)

The GFM DI Prototype makes additional org structure and identity attributes available for use in ABAC

Current EIAS Attributes

Segment	Name
Person (1:1)	DOD EDI
	Enterprise User Name
	US Citizenship Status Code
	Country Of Citizenship
	JPAS Eligibility Code
Persona (1:N) HR - Personnel	Persona Type Code
	Persona Display Name
	DoD Association Code
	Administrative Org Code
	Pay Plan
	Pay Grade
	Duty Occupational Code
	Primary Occupational Code
	JPAS Access Code

GFM Org and Identity Attributes

Persona (1:N) HR - Manpower	Billet OUID
	Billet Service Affiliation
	Billet Component Affiliation
	EDIPI-to-OUID Start Date
	EDIPI-to-OUID End Date
	Billet Pay Grade
	Billet Primary Skill/Specialty
	Organizational Structure Relationships (e.g., the ADCON FMID Above List)

QUESTIONS ?